DEPARTMENT OF COMMERCE

DEFENSIVE TRAVEL BRIEFING

PURPOSE

As a Commerce employee, you have access to critical U.S. government information. The purpose of this briefing is to ensure that you understand your responsibilities to protect the information, and to make you aware of security vulnerabilities associated with foreign travel.

Presidential Decision Directive/NSC-12 "Security Awareness and Reporting Foreign Contacts", requires security personnel to establish and maintain security awareness programs which include formal briefings of the threat posed by foreign intelligence services. The awareness program must focus on the intelligence gathering of classified as well as other sensitive information. This Defensive Travel Briefing is part of Commerce's Security Awareness Program.

APPLICABILITY

This defensive travel briefing is required by DAO-207-1. When traveling abroad, Departmental personnel, including summer hires, those on temporary assignment, and contractors are required to receive an annual defensive travel briefing. Any individual returning from travel of 90 days or more must undergo a security debriefing upon their return to the U.S.

AREAS OF INTEREST

Within the Department, we possess a wealth of information of interest to foreign powers and entities. Information regarding the Export Administration Act, ongoing negotiations, trade issues, economic indicators, industrial resources, production capabilities, manufacturing and other critical technologies, satellite data, telecommunications and computer science information, as well as numerous other types of sensitive information may be sought. Because of your access to personnel, facilities, and information, YOU, as a Commerce employee, present an opportunity for a foreign entity to expand their knowledge about U.S. technology, capabilities and vulnerabilities. The information contained in this briefing regarding possible intelligence collection may occur in countries with which we are allies. For that reason, we ask you to be alert to your surroundings and aware of your actions at all times wherever you travel internationally.

THE NATIONAL SECURITY THREAT LIST

The FBI considers the following to be threats to our national security regardless of the country involved:

Any foreign intelligence activity which is:

* Targeting U.S. intelligence and foreign affairs information and U.S. Government Officials

* Directed at critical technology

* Directed at the collection of U.S. industrial proprietary economic information

* Directed at the collection of information relating to defense establishments and national preparedness

* Involving the proliferation of special weapons of mass destruction

* Involving perception management and active measures

If you become aware of or suspect any foreign intelligence activity aimed at the above list notify your Security Officer.

PRIOR TO DEPARTURE

1. Contact your Regional Security Officer (757-441-3431/3428/3620) to obtain the most recent travel advisory information. You may also want to contact the Department of State recorded messages at 202-647-5225.

2. Carefully complete your Visa application, as it will be scrutinized. If you are a naturalized U.S. citizen returning to the country of your origin, your citizenship may be questioned. If you encounter such a problem, please contact the State Department for guidance.

3. Ensure that items you carry with you are not controversial or prohibited. Political material or anything that could be considered pornographic should not be carried. If you carry prescription drugs with you, be certain that they are clearly marked and bring only necessary quantities.

4. Carrying letters, packages or gifts to individuals in other countries should be avoided. You may be viewed as a courier attempting to bring the material for subversive or illegal purposes.

5. DO NOT TAKE CLASSIFIED MATERIAL with you as you travel. Arrange to have the material transmitted by other means prior to your departure. Consult with your Security Officer for guidance.

6. Limit the amount of identification that you take. If you have several forms of Government ID (i.e. Commerce ID, building pass, courier card), bring only one ID with you. Make a photocopy of any ID or credit card you will be bringing and leave the copy at home. Write down your passport number and keep it separate from your passport. Do the same with your address and telephone.

7. The carrying of laptop computers is discouraged, but not prohibited. Consult your Security Officer and your Information Technology Security Officer if you plan to take laptop.

UPON ARRIVAL

1. An accurate declaration of all money and valuables should be made at entry. Some countries give the traveler a copy of the declaration, which must be surrendered upon leaving. It is important to keep receipts of all money exchanges; these frequently are required upon departure. Undeclared sums of U.S. or other currency are likely to cause difficulty with authorities and may be confiscated upon departure.

2. Declare such items as cameras, radios, etc., to preclude possible explanations, customs charges, or confiscation when you leave.

3. Contact the American Embassy or Consulate prior to your arrival, and provide your local address and the probable length of your visit. For most official business visits a cable should be sent to the appropriate Embassy advising of your visit.

4. Use of public transportation is recommended rather than driving yourself, because involvement in traffic accidents can be problematic. Taxis are the preferred mode of transportation. State Department travel advisories provide updated information regarding public transportation concerns in the country you are visiting.

YOUR ACTIVITIES AND BEHAVIOR

1. In all of your activities, show discretion and common sense. MAINTAIN A LOW PROFILE. Refrain from any behavior that may make you conspicuous or a potential target. NEVER engage in any illegal activity, excessive drinking or gambling. Use your best judgement to carefully avoid any situation, which may allow a foreign intelligence agency the opportunity to coerce or blackmail you.

2. Do not discuss classified or sensitive information in any vehicle, restaurant, hotel room, hotel lobby, or other public place. In any public place, your conversation may be

overheard, or you may be monitored. If you need to call the U.S. to discuss classified or sensitive information, locate a secure telephone by contacting the Regional Security Officer at the U.S. Embassy.

3. If you locate any possible surveillance equipment, such as microphones, telephone taps, miniature recording devices, or cameras, do not try to neutralize or dismantle it. Assume the device is operable and that active monitoring is ongoing. Report what you have found to the U.S. Embassy or Consulate. When you return, advise your security officer.

4. Never leave luggage or briefcases that contain classified or sensitive information unattended. This includes leaving your briefcase in your hotel room. We encourage you to keep your briefcase containing sensitive information, immediately in your possession. Departmental personnel frequently report occurrences of their luggage or briefcase being searched or rummaged through. If this happens to you, report the incident to your Security Officer when you return.

5. Foreign Intelligence Services may place you under physical surveillance or you may suspect that you are being watched. It is better to ignore the surveillance than attempt to lose or evade it. In any event your actions should be prudent and not likely to generate suspicion. Good precautionary measures are to use well traveled highways and avoid establishing routine schedules.

6. Never try to photograph military personnel, installations, or other "restricted areas". It is best to also refrain from photographing police installations, industrial structures, transportation facilities and boarder areas.

7. Beware of overly friendly or solicitous people that you meet. Do not establish personal or intimate relationships with these individuals as they may be employed by the intelligence service. Do not share any work-related information with any person who does not have a need to know.

8. Do not accept packages and agree to transport them back to the U.S. Even if your friends, relatives, and professional contacts, make the request, do not accept the package.

9. If you will be on an extended visit and expect to be writing or receiving mail, remember that it may be subjected to censorship. Never make references to any classified or sensitive information.

10. Avoid any areas where there is political or ethnic unrest, demonstrations or protests.

11. Should you be detained or arrested for any reason by the police or other officials, be cooperative, and contact the U.S. Embassy or Consulate immediately. Do not make any statements or sign any documents you do not fully understand until you have conferred with an Embassy representative.

12. Do not leave documents in hotel safes.

13. You may keep this document for reference, but do not carry it with you.

UPON YOUR RETURN

Contact your Security Officer to report foreign contacts and any unusual incidents. You must receive a security debriefing if you have been abroad for more than 90 days. You are required to report all contacts with individuals of any nationality, either within or outside the scope of your official activities in which:

*Illegal or unauthorized access is sought to classified or sensitive information

* You are concerned that you may be the target of an actual or attempted exploitation by a foreign entity.

EMERGENCY NOTIFICATION PHONE NUMBERS

Before your departure, it is recommended that you provide your family and/or a close friend with the name and phone number of your supervisor or coworker so that you can be reached in the event of an emergency.

If an emergency does occur, persons needing to reach you should be instructed to contact you via your immediateoffice. If this is not possible, the 24-hour State Department Operations Center at 202-647-1512, may be able to assist others in reaching you.

DEPARTMENT OF COMMERCE
DEFENSIVE TRAVEL BRIEFING
ACKNOWLEDGEMENT CERTIFICATE

My signature below indicates that I have read/been briefed and understand the Department of Commerce, Office of Security Defensive Travel Briefing. I am aware that any questions I have concerning the contents of this briefing should be directed to my Regional Security Officer.

PRINT NAME: _____

SSN: _____

BUREAU/OFFICE: _____

TRAVEL DATE(S): _____

COUNTRY(S)/REGION: _____

PURPOSE OF VISIT: _____
_____

WORK PHONE _____

_____
SIGNATURE / DATE

Collection of this information is authorized by Executive Order 9397, 10450, 12356, U.S.C. 301 and 7531-532; 15 U.S.C. 1501 et seq; AND 44 U.S.C. 3101

Please forward this signed page to the following:

DEPARTMENT OF COMMERCE
EASTERN REGIONAL SECURITY OFFICE
NORFOLK FEDERAL BUILDING
200 GRANBY STREET, ROOM 407
NORFOLK, VA 23510
Fax (757) 441-3422